QUANTUM COMPUTING

MGS 2025 - Sheffield

Venanzio Capretta

LECTURE 5:
- Quantum Computing with Oracles
- Grover's Search Algorithm

QUANTUM COMPUTING WITH ORACLES

An <u>oracle</u> is a Boolean function on a number of bits (classical)

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

Idea: we are doing a search on a set of items (N items)
encoded in n-bit sequences ($N \leq 2^n$)
f tells us if an item satisfies our search criteria

Classical solution: test each item until you find the solution,
linear complexity in N, exponential in n

Quantum idea: Apply f to a superposition of all sequences

First we must turn f into a quantum (unitary) operator.
Assuming $f(y)=1$ for exacty one sequence y, we define a unitary U_f such that:

$$U_f\,|x\rangle = \begin{cases} -|y\rangle & \text{if } f|x\rangle = 1 \\ |x\rangle & \text{otherwise} \end{cases}$$

there are techniques to do this efficiently

The matrix representation of U_f is:

$$U_f = \begin{bmatrix} 1 & & & & \textcircled{0} \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ & & & & 1 \\ \textcircled{0} & & & & \ddots \\ & & & & & 1 \end{bmatrix}$$

position corresponding to y

But we never explicitely compute this matrix representation

Instead we use techniques to translate a Boolean algorithm to a quantum circuit

To compute the solution: start with a maximally superimposed state:

$$|\Psi\rangle = H^{\otimes n} |\bar{0}\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle_n$$

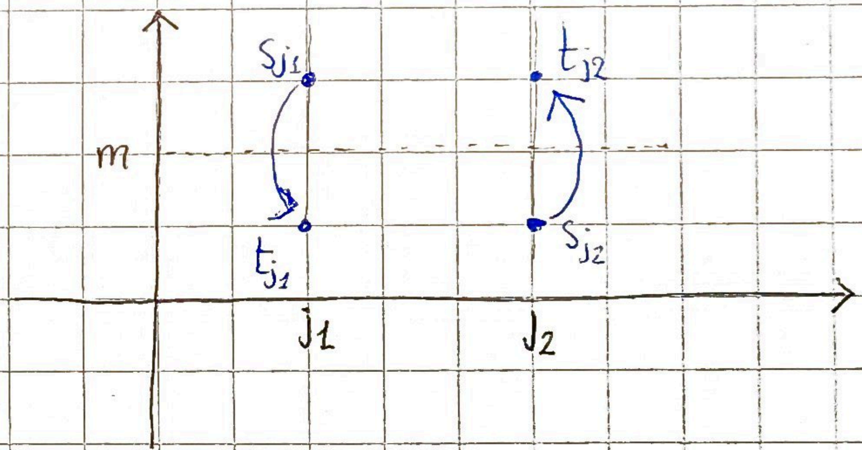
If we measure the state now, every sequence has the same probability $\left(\frac{1}{2}\right)^n$

Instead we will iterate an operator based on U_f to boost the amplitude of the correct sequence

INVERSION ABOUT THE MEAN

Let $S = \{s_j\}_j$ be a set of real values, with mean $m = \sum s_j / N$

Set $T = \{ t_j = 2m - s_j \}_j$ (inversion about the mean)



We have:

- The mean is still m
- If $s_j = m$, then $t_j = m$
- $t_j - m = m - s_j$, so $|t_j - m| = |s_j - m|$
- If $s_j > m$, then $t_j < m$; if $s_j < m$, then $t_j > m$

We apply a quantum version of inversion about the mean

GROVER DIFFUSION OPERATOR: for $|\Psi\rangle = H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{2^n}}\sum_j |j\rangle_n$

$$U_\Psi = 2\underbrace{|\Psi\rangle\langle\Psi|}_{\text{this is the "mean"}} - \mathbb{1}_{2^n}$$ inversion about the mean

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}}\begin{bmatrix}1\\ \vdots \\ 1\end{bmatrix} \qquad |\Psi\rangle\langle\Psi| = \frac{1}{2^n}\begin{bmatrix}1\\ \vdots \\ 1\end{bmatrix}\begin{bmatrix}1 & \cdots & 1\end{bmatrix} = \frac{1}{2^n}\begin{bmatrix}1\end{bmatrix}_{i,j}$$

density matrix of $|\Psi\rangle$

Applying $|\Psi\rangle\langle\Psi|$ to a vector $[a_j]_j$ we obtain a vector with the mean in every position:

$$\left(|\Psi\rangle\langle\Psi|\right)\begin{bmatrix}a_0\\ \vdots \\ a_{2^n-1}\end{bmatrix} = \frac{1}{2^n}\begin{bmatrix}\Sigma_j a_j\\ \vdots \\ \Sigma_j a_j\end{bmatrix} = \begin{bmatrix}m\\ \vdots \\ m\end{bmatrix}$$

where $m = \left(\Sigma_j a_j\right)/2^n$ is the mean

So $U_\psi = 2|\psi\rangle\langle\psi| - \mathbb{1}$ is the "inversion about the mean"

$$U_\psi [a_j]_j = [2m - a_j]_j$$

Grover operator: $G = U_\psi \cdot U_f$

Idea: iterate G (starting with a vector with equal entries) to boost the coefficients of the correct solution(s)

Algorithm:
- Start with the input qubits in a uniform superimposed state
  $H^{\otimes n} |0\rangle_n$
- Iterate G an optimal number of times ...
- Measure the result
  there will be a high probability (close to 100%) of observing the correct solution

The "optimal number of iterations" is: ($N=2^n$)

- $\frac{\pi}{4}\sqrt{N}$ if there is exactly one correct solutions
- $\frac{\pi}{4}\sqrt{\frac{N}{M}}$ if there are M solutions
- If we don't know the number of solutions,

  we must first run an algorithm to estimate M (quantum counting)

The operator G <u>does not converge asymptotically</u>

if you iterate it more than the optimal number of times
you will move away from the solution

SHOR ALGORITHM

Fast factorization of integers, $O(n^2 \log n)$

breaks RSA

Based on the Quantum Fourier Transform,

exponentially faster thaan FFT